

# The Digital Services Act

## A Guide for Decentralized Services

Activity Pub



# Section I: The Digital Services Act - Regulating the Fediverse

The [Digital Services Act](#) (DSA) is a new law in the European Union that seeks to address illegal content online, empower users to report content and contest platforms' decisions, and ensure transparency and consistency in the content moderation space.

**The Digital Services Act applies to all online intermediaries (including public Fediverse servers) that offer their services within the European Union as of February 17, 2024.**

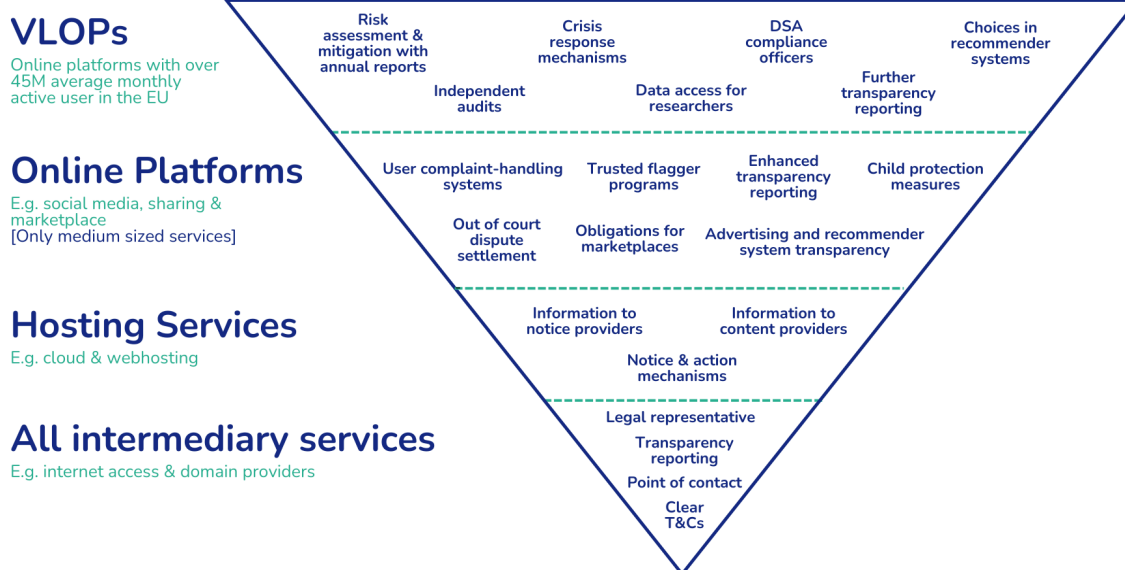
## *Who does this affect?*

When it comes to who - and what - falls in the scope of the DSA, we can consider it as an umbrella covering all online intermediaries involved in providing access to, hosting, transmitting, and indexing content created by others. The DSA categorizes online services into five distinct groups, each with different obligations associated with them:

- **Conduit Services:** Think of these as the internet's highways, facilitating the seamless flow of information across the digital landscape. These include internet exchange points, wireless access points, DNS services, and virtual private networks.
- **Caching Services:** These services temporarily store data to make our online experience faster and more efficient. Content delivery networks, reverse proxies, and content adaptation proxies fall into this category, working behind the scenes to streamline content transmission.
- **Hosting Services:** The types of services where content is not just stored but shared upon request, for example, web-hosting, file-hosting or sharing platforms.
  - **Online platforms:** hosting services that publicly share user-generated content, encompassing everything from social media to online marketplaces, gaming platforms, and video platforms
  - **Very large online platforms:** online platforms that publicly share user-generated content and have more than 45 million users within the EU.

In addition to the categories of providers, different obligations are applicable depending on the size of the platform. **Micro and small platforms**, those below **10 million euros in their turnover or balance sheet AND less than 50 employees** are exempt from transparency obligations and additional obligations applicable to online platforms.

The “flipped pyramid” below provides an overview of the obligations that vary by service type and size.



**Ok - but what about decentralized services, where do we sit?**

Independently hosted servers or instances across decentralized social networks like Mastodon, PeerTube, and Pixelfed align best with the EU DSA’s definition of an online platform, which is a hosting service that also makes user-generated (not curated) content available to the public.

Most instances across decentralized networks are likely to be classified as Small and Micro Enterprises (SMEs). The categorization reduces the obligations normally applicable to online platforms and allows for smaller services to only worry about a select number of obligations. Classifying your instance as a small or micro online platform is based on the assumption that your server doesn’t currently employ more than 50 people **and** doesn’t have an annual turnover or balance sheet of more than 10 million euros. If you surpass these thresholds or are concerned it might be you in the future, we can refer you to [this guide](#) for a broader suite of obligations under the DSA.

**What does the DSA say about liability?**

The DSA maintains the well-known limited liability regime online. In simple terms, services are not liable for content unless they have been notified of its presence.

Platforms can therefore be held liable for such content when they have specific knowledge of its presence and fail to remove it promptly. The mere potential for illegal content to exist on a platform does not constitute liability - knowledge has to be specific.

Further, similar to the Good Samaritan principle in the US, platforms are not held liable purely for proactively searching for and removing illegal content. Platforms remain free to monitor their spaces, facing liability only in specific scenarios such as knowingly hosting illegal content or not responding swiftly enough upon being alerted.

While you are protected from general liability, the DSA does set out a number of legal obligations on platforms for which compliance will be monitored by the European Commission and Digital Services Coordinators across Europe.

## Section II: What does the DSA require from me?

This section is intended to break down the DSA requirements that apply to you and your instance. As a small or micro online platform, for now, you're exempt from some of the more resource-intensive obligations (don't worry - transparency reporting isn't a requirement until you've hit the medium status!). Let's take a look at the nine provisions you'll need to understand and implement in order to be compliant with the DSA. Scroll further for specific examples and templates in Section III to help bring these requirements to life. *For a list of obligations you might hear about but do not apply to you unless you reach a medium size platform status, see the table in Annex I.*

### ***Sounds straightforward enough - but who's checking up on this?***

The enforcement framework of the DSA is centered around Digital Services Coordinators (DSCs) across each Member State. These DSCs are tasked with monitoring online platforms within their jurisdiction to ensure their compliance with their respective obligations. As an online platform, you must be prepared to cooperate with DSCs and provide information upon request, or implement changes to your policies based on feedback. You'll typically hear from the DSC where you are based or where you have a legal representative. If you are not in Europe and do not appoint a legal representative, any DSC can get in touch and enforce the rules. A [list of designated DSCs](#) is available online.

Article and Provision	Explanation
<b>Article 9: Orders to Act Against Illegal Content</b>	From time to time, you may receive an order from authorities informing you of specific illegal content on your instance and requesting its removal. When this happens, the DSA requires you to quickly inform the authorities about the actions taken in response. The order you might receive will clearly state why the content is illegal and provide precise information to locate the content.
<b>Article 10: Orders to Provide Information</b>	Occasionally, authorities may require information about users linked to illegal activities or content, and Article 10 requires you as an instance owner to comply. These orders will have to detail the legal grounds, and specify the needed information.
<b>Article 11: Points of Contact for Authorities</b>	All servers must establish a direct contact point for EU authorities, making this information public and specifying the acceptable communication languages. This aims to support efficient communication between instances and authorities, facilitating quick responses to legal and safety issues.
<b>Article 12: Points of Contact for Users</b>	Similarly, there must be an easily accessible method for users to contact their instance administrator, ensuring users have a way to report issues or illegal content.
<b>Article 13: Legal Representatives</b>	Instances established outside the EU that serve EU users or make their services available in the EU are required to have an EU-based legal representative to manage compliance and communication with EU authorities.
<b>Article 14: Terms and Conditions</b>	Instances must clearly communicate any content restrictions, moderation policies and processes, and overall guidelines on prohibited content and conduct in simple language.
<b>Article 16: Notice and Action Mechanism</b>	Instances are required to implement a straightforward system for users to report illegal content, with a form for users to provide detailed and precise reports.
<b>Article 17: Statement of Reasons</b>	When content is moderated - whether that's a freeze, limitation, or suspension - servers must issue a clear explanation to the affected user, outlining the decision.
<b>Article 18: Notification of Suspicions of Criminal Offences</b>	If an instance becomes aware that a criminal offense with a threat to life or safety has been, is being, or will be committed, it is obliged to alert law enforcement. This includes a range of crimes such as human trafficking, terrorism, and CSAM.

## Section III: Practical Implementation of the DSA to Achieve Compliance

As an administrator, there are several core features of instances which can be customized and updated to achieve compliance. These include instance rules, community management tasks such as enforcing rules and moderating content, and implementing tools or avenues for reporting content. While this will vary across Mastodon, Pixelfed, PeerTube, or MissKey interfaces, this section takes a look at how the core DSA requirements can be applied.

Articles 9-10: Official requests from authorities	
Requirement	Guidance
<p><b>Act against illegal content or provide information when notified by an authority</b></p>	<p>Upon receiving an official request to act against illegal content or provide information, there are several steps you can take to ensure the request is legitimate. First, you can check the sender's email domain - does it match the specific police force or authority's official site?</p> <p>Next, ensure the request contains the following information:</p> <ul style="list-style-type: none"> <li>• <b>Legal Basis:</b> A reference to the specific Union or national law that forms the basis of the order.</li> <li>• <b>Reasoning:</b> A detailed explanation of why the content is considered illegal or why information is being requested, citing specific provisions of Union law or national law that align with Union law.</li> <li>• <b>Issuing Authority:</b> Information identifying the authority that issued the order.</li> <li>• <b>Content Identification:</b> Clear details to help you locate the illegal content, such as one or more exact URLs and, if needed, additional information.</li> <li>• <b>Redress Mechanisms:</b> Information about the ways you (as the service provider) and the content creator can contest the order or seek further clarification.</li> <li>• <b>Authority for Reporting Compliance:</b> If applicable, details on which authority should be informed about the actions you've taken in response to the order.</li> </ul> <p>For one example of an official EU removal request, see <a href="#">Annex I</a> in the EU Regulation on the Dissemination of Terrorist Content 2021/784.</p>


Articles 11-12: Point of contact for authorities and users	
Requirement	Guidance
<p><b>Designate a single point of contact for relevant authorities and users</b></p>	<p>Every instance should designate a single point of contact for users and relevant authorities, whether it's an administrator, moderation team, or a dedicated contact person. This ensures efficient communication and coordination, especially for responding to legal notices. For operational ease, these points of contact should be separate email addresses - one dedicated to your users, and the other for authorities.</p> <p>Instance administrators can include this information in the "About" section of the instance, where any current points of contact for DMCA or GDPR are listed.</p>

**Example**

**example.social**

Decentralized social media powered by Mastodon

ADMINISTERED BY:



example-admin  
@admin

CONTACT:

member-help@example.social

▼ About

**Welcome to Example.Social!**

- Technical Support: [member-help@example.social](mailto:member-help@example.social)
- Moderation Appeals: [moderation@example.social](mailto:moderation@example.social)
- Legal/Regulatory/Compliance: [legal@example.social](mailto:legal@example.social)

*Screenshot from the About section of a Mastodon server*

Article 13: EU-based legal representative	
Requirement	Guidance
<p><b>Appoint a legal representative in the EU</b></p>	<p>If your service is accessible to users in the EU but you don't have an establishment there, you're required to designate either a legal or natural person as your legal representative within one of the Member States where you offer services. Your legal representative will act on your behalf for interactions with the EU's Member States'</p>

	<p>authorities, regarding compliance with and enforcement of the DSA. You must notify the Digital Services Coordinator in the Member State of your representative's name, postal address, email address, and telephone number. Ensure this information is public, easily accessible, accurate, and regularly updated. Most legal representative services do not offer an affordable option for donation-driven services. IFTAS is researching ways to offer this service, but in the meantime, we strongly recommend you ensure you have added a designated contact for authorities to reach you.</p>
--	---

Articles 14: Terms and Conditions	
Requirement	Guidance
<p><b>Publish clear Terms and Conditions (T&amp;Cs) and understandable information on the content moderation tools and processes</b></p>	<p>Instances should publish clear and understandable Terms and Conditions which can be supplemented by Community Guidelines that outline acceptable behavior, prohibited content, and the moderation process, including if any third-party moderation APIs are used. What constitutes a freeze, limitation, or suspension of accounts? Why and how does this server not federate with certain others? Are any third-party tools used to moderate content?</p> <p>These rules should be easily accessible to users and prominently displayed on the instance's interface (i.e., on your About page). You should let your users know whenever you update or change your rules, for example via a Notice on the Status page.</p>

Example
<p>You might find these examples helpful: <a href="#">Dailymotion</a>, <a href="#">Discord</a>, <a href="#">Roblox</a>, or some sample text below. You can also take a look at the <a href="#">About section of IFTAS's sandbox server</a> for an example.</p> <p style="text-align: center;">Welcome to [Your Instance Name]! To ensure a safe environment for all, we've established some key rules and guidelines, especially around content moderation.</p> <ol style="list-style-type: none"> <li>1. Content Moderation Policies             <ol style="list-style-type: none"> <li>a. Our instance prohibits:</li> </ol> </li> </ol>



- Illegal content as per EU laws and local regulations.
  - Infringement of intellectual property rights or personal privacy.
- b. Moderation Tools and Measures:
- Content Warnings (CW): Users must apply CWs to sensitive content to inform others before viewing.
  - Account Isolation: In cases of severe rule violations, we may isolate accounts. Isolation means that your ability to interact with others on the platform will be restricted.
  - Suspension: Accounts that repeatedly or severely violate our rules may be suspended from our service. We reserve the right to apply a temporary or permanent suspension

## 2. Changes to Terms and Conditions

We commit to notifying you of any significant changes to these rules. Updates may be communicated through platform announcements or in our Notice Updates.

## 3. Fair and Objective Enforcement

We aspire to make all content moderation decisions diligently and objectively. To this end, we have regard to the fundamental rights of our users (such as the right to free expression) and the principle of proportionality.

We rely on community moderation, human review, and [if applicable] automated tools

## 5. Contact and Feedback

For questions, clarifications, or to report violations, please reach out to us at [contact information]. We're dedicated to maintaining a positive and respectful space for everyone in our community.

### Articles 16: Notice and action mechanisms

Requirement	Guidance
<b>Create notice and action mechanisms for users to report content that is illegal</b>	Instances should integrate user-friendly reporting mechanisms for users to report illegal content. This can be achieved by implementing or enhancing existing built-in reporting features within the server interface, allowing users to submit detailed reports including the content's URL and reasons for reporting.

	<p>You should also send the reporting user a confirmation of receipt of their report, and notify them of whatever enforcement action is taken. If you use an automated tool for processing or decision-making, be clear about that, too.</p>
--	--

**Example**

**Illegal Content Report Form**

Welcome to our legal request submission portal. We are committed to protecting user privacy and will only release non-public information about our users to law enforcement authorities in response to appropriate legal processes, such as subpoenas, court orders, or search warrants, or in response to valid emergency requests.

This content violates the laws in (please select a country)

Country ▾

Enter the legal reason for your report

Legal Reason For Your Report ▾

Enter your name

Your Name

Enter your email

Your Email

Enter the reason for your report

Reason for Report

Please check this box to confirm you are acting in good faith and have reported the content truthfully and accurately

*Screenshot of a Content Reporting Form from Nima, the Trust & Safety platform by Tremau*

Articles 17: Statement of reasons (SoR)	
Requirement	Guidance
<p><b>Send a statement of reasons to the affected user after taking action against content or an account</b></p>	<p>After taking action against an account or content, administrators should inform the user via email of the action taken and provide a statement of reasons as to why the content or account is restricted or disabled. The statement of reasons should also include information on the possibilities available to appeal the decision. Our template below includes the minimum requirements.</p>

### Example

#### Subject: Notice of Action Taken on Your Content/Account

Dear [User's Name],  
 We're reaching out to inform you of an action we've recently taken on your content/account in accordance with our platform's policies [and the Digital Services Act (DSA)]. Please find the details of this action below:

#### Type of Restriction Imposed:

[Isolation of content / Disabling access to content / Restriction of content visibility / Suspension of monetary payments / Suspension or termination of service / Suspension or termination of account]

#### Effective Date and Duration:

[Date of imposition]  
 [Duration of the restriction, if applicable]

#### Reasons for the Decision:

[Specify whether the decision was based on illegal content, violation of terms and conditions, a notice submitted in accordance with Article 16, or voluntary investigations]  
 [Legal or contractual grounds for considering the content illegal or incompatible with our terms]  
 [If applicable, information about the use of automated means in the decision-making process]

#### Territorial Scope:

[If applicable, specify the geographical scope of the restriction]

We understand that this may be disappointing news. Our goal is to maintain a safe environment for all users while respecting your rights and freedoms.

Sincerely,  
 [Your Platform's Name]

### Articles 18: Notification of suspicions of criminal offenses

Requirement	Guidance
<p><b>Create a mechanism to notify law enforcement of serious criminal offenses to life or safety and report such content to appropriate law enforcement or judicial authorities in the Member State(s) concerned.</b></p>	<p>Instances should have a narrow taxonomy of “serious criminal offences”, including crimes such as human trafficking, sexual abuse and exploitation of children, child pornography and terrorism. The primary objective is to prevent the loss of life or serious injury. To assess whether a suspicion is reasonable, you should consider some credibility criteria, addressing questions such as:</p> <ul style="list-style-type: none"> <li>• <i>Is the information reported clear enough? Can it constitute a solid base for action?</i></li> </ul>

<p>Please note that this includes potential future offenses, not just past ones.</p> <p><i>No example can be provided for Article 18 as it relates to an internal process so platforms haven't released any public documents.</i></p>	<ul style="list-style-type: none"> <li>● <i>Is the reporting source reliable?</i></li> <li>● <i>Can the reported information be verified with known facts?</i></li> <li>● <i>Is there any conflict of interest for the reporter?</i></li> <li>● <i>Does the reporter have a track record of making false or baseless claims?</i></li> <li>● <i>Has the information been timely reported?</i></li> </ul> <p>Simply put, it's best to report crimes to the authorities in the country where the crime occurred. If it's unclear which country to report to due to issues like wrong information or unclear location, instances can also report to the authorities in the country where the suspect or victim lives. If you're still unsure, Europol is the default option, along with the authorities where the instance is established. To get ready to report content, you may contact Europol or your Digital Services Coordinator to receive a contact list of relevant authorities.</p>
---	--

For administrators of platforms like Mastodon, PeerTube, and Pixelfed, the challenge now lies in navigating the DSA in a way that is both compliant and conducive to the open, community-driven ethos that defines the Fediverse. The guidance provided above aims to demystify the DSA's requirements and offer practical advice on achieving compliance without compromising the unique qualities that make decentralized social networks a valuable alternative to their counterparts. As we move forward and new regulation comes into force, it is essential to understand what your minimum compliance obligations are.

About IFTAS: IFTAS is a charitable nonprofit committed to fostering a safer, more inclusive open social web by empowering volunteer moderators with the tools, resources, and support necessary to navigate the complexities of digital content moderation. If you'd like to learn more, visit [about.iftas.org](https://about.iftas.org).

*The materials provided are for general informational purposes only. These materials do not, and are not intended to, constitute legal advice, and you should not act or refrain from acting based on any information provided. Please consult with your own legal counsel on your situation and specific legal questions.*

## Annex I

As micro and small platforms, most instances are currently (as of March 2024) likely exempt from compliance with the DSA provisions listed below. Nevertheless, it is important to be aware of these articles as they may become relevant to you in the future.

Article and Provision	Explanation
<b>Article 15: Transparency reporting obligations for providers of intermediary services</b>	Publish, at least once a year, an easy-to-read report detailing all content moderation activities undertaken within the year. It should include all the information about orders to act or provide information (Articles 9 and 10), notices received from users and subsequent actions (Article 16), complaints received through internal systems and the actions addressed in response (Article 20), and the deployment of any own-initiative or automated tools for content moderation. The European Commission has published a <a href="#">delegated act</a> outlining the types of moderation to be transparent about as well as other practical guidelines on building a transparency report compliant with the DSA.
<b>Article 20: Internal complaint-handling system</b>	Offer users access to an internal complaint handling system to contest any moderation decision. This system should be freely available for users for at least six months from the time they are notified of the initial decision. If an error was made, the content or account should be restored.
<b>Article 21: Out-of-court dispute settlement</b>	Inform users of the possibility of accessing an out-of-court dispute settlement body to solve pending issues. These bodies are certified by DSCs and their decisions are not binding.
<b>Article 22: Trusted flaggers</b>	Prioritize the moderation of notices submitted by trusted flaggers, which are entities certified by DSCs based on their expertise and independence.
<b>Article 23: Measures and protection against misuse</b>	Suspend your services for users who frequently either provide clear illegal content or submit clear unfounded notices or complaints. You should explain the policies for these actions in your terms and conditions.
<b>Article 24: Transparency reporting obligations for providers of online platforms</b>	In your transparency reports, include information about disputes submitted to the out-of-court dispute settlement bodies (Article 21) and the number of suspensions imposed (Article 23). Additionally every six months, you should publicly share the number of average monthly active users in the EU.
<b>Article 25: Online interface design</b>	The design of your interfaces should not deceive or manipulate the user's ability to make free decisions.
<b>Article 26: Advertising on online platforms</b>	If you serve advertisements on your service, you must disclose its nature, the entity on whose behalf it is displayed, who funds it, and the targeting criteria used.
<b>Article 27: Recommender system transparency</b>	If you operate a recommender system, you are obliged to outline parameters of your algorithmic recommendation systems in your Terms and Conditions. Additionally, provide users with instructions on how to modify these criteria to tailor their experience.
<b>Article 28: Protection of minors</b>	Ensure an adequate level of privacy, safety and security for minors and prohibit the display of any advertisements that utilize their personal data.